General Services Administration
Information Security Oversight Office
Washington, DC 20405

80-062

RMD
80-131

DD/A Regist
80-018

14 JAN 1980

Admiral Stansfield Turner, USN
Director
Central Intelligence Agency
Washington, DC 20505

Dear Admiral Turner:

Section 3-403 of Executive Order 12065, "National Security Information," authorizes the Secretary of Defense to establish special procedures for the systematic review and declassification of classified cryptologic information. Further, Section III.C.2.d. of Information Security Oversight Office Directive No. 1 provides that such procedures promulgated in accordance with the provisions of Section 3-403 of the Order shall be binding on all departments and agencies.

By enclosure to our letter of October 4, 1979, we distributed to you a copy of such procedures. The document entitled, "Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065," bears a National Security Agency letterhead and is dated September 1979.

Attached herewith is a copy of revised procedures dated January 1980 which supersede the ones mentioned above. Please insure that all appropriate personnel/activities are furnished copies of the revision and that, where possible, all superseded copies be destroyed.

Sincerely,

Robert W. Wells

ROBERT W. WELLS
Acting Director

Enclosure

OFFICE OF THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

POLICY

January 1980

SPECIAL PROCEDURES FOR USE IN SYSTEMATIC REVIEW OF CRYPTOLOGIC INFORMATION PURSUANT TO SECTION 3-403 OF EXECUTIVE ORDER 12065

1. General guideline: cryptologic information uncovered in systematic review for declassification of 20/30 year old government records is not to be declassified by other than U.S. government cryptologic agencies. The information may concern or reveal the processes, techniques, operations, and scope of signals intelligence comprising communications intelligence, electronics intelligence, and telemetry intelligence, or it may concern the cryptosecurity and emission security components of communications security, including the communications portion of cover and deception plans.

2. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

a. Those that relate to communications security (COMSEC). In documentary form, they provide COMSEC guidance or information. Normally, COMSEC documents and materials are accountable under the "Communications Security Material Control System." Examples are: items bearing "TSEC" nomenclature ("TSEC" plus three letters), "Crypto Keying Material" for use in enciphering communications, Controlled COMSEC Items (CCI), and cryptographic keying devices.

b. Those that relate to signals intelligence (SIGINT). These appear as reports in various formats that bear security classification, sometimes followed by a five-letter codeword (World War II's ULTRA, for example) and often carry warning caveats such as "This document contains codeword material," "Utmost secrecy is necessary . . . ." Formats will appear, for example, as messages having addresses, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

c. Research, development, test, and evaluation reports and information that relates to either COMSEC or SIGINT.

3. Commonly used words that may help in identification of these documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

4. Special procedures apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information:

a. COMSEC Documents and Materials. If records or materials in this category are found in agency or department files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency or department concerned or by appropriate channels to the following address:

Director, National Security Agency/
Chief, Central Security Service
ATTN: Policy Staff
Fort George G. Meade, MD 20755

b. SIGINT Information.

(1) If the SIGINT information is contained in a document or record originated by a U. S. government cryptologic organization and is in the files of a non-cryptologic agency or department, such material will not be declassified. The material may be destroyed unless the holding agency's approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the originating organization for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency or department into documents it produces, referral of the SIGINT information to the originator is necessary prior to any declassification action.